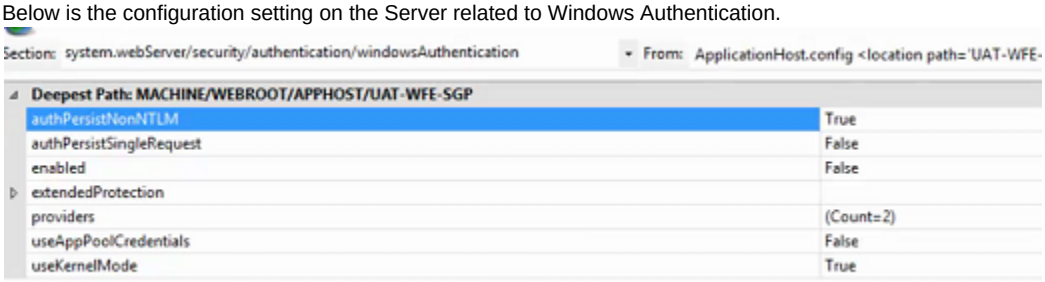
Windows Authentication Issue

🤔 Problem

Unable to do Windows Authentication while accessing the Application.

🌱 Solution

Below is the configuration setting on the Server related to Windows Authentication.



`authPersistNonNTLM`	Optional **Boolean** attribute. Specifies whether IIS automatically reauthenticates every non-NTLM (for example, Kerberos) request, even those on the same connection. **False** enables multiple authentications for the same connections. **Note:** A setting of **true** means that the client will be authenticated only once on the same connection. IIS will cache a token or ticket on the server for a TCP session that stays established. The default is `false`.
`authPersistSingleRequest`	Optional **Boolean** attribute. Setting this flag to **true** specifies that authentication persists only for a single request on a connection. IIS resets the authentication at the end of each request, and forces reauthentication on the next request of the session. The default value is `false`.

Configuration on the APV was not compatible with above mentioned Settings on the Application and due to this Users were not able to do Authentication or not able to access the application properly.

With Default configuration on APV: i.e. having “HTTP Authsplice on <Virtual Service>” CLI, Server was authenticating the Users, however, subsequent request after the Login were being forwarded to same server and this was creating an issue.

Because, for all the initial requests, Server was Responding with HTTP Response “401 unauthorized” and due to this, APV thinks that, all the requests from the Client may require Authentication and will be forwarded to same server without going into SLB lookup (Checking the Policies or Group Methods) Process.

Due to this, users were not able to access the Subsequent requests post login or Authentication.

Hence In order to fix this, we were supposed to disable the “http authsplice off <virtual Service>”.

However, Post making this, users were not able to login into application as “APV was using different TCP connections” to forward the Authentication requests (Request, NTLMSSP-Negotiate, NTLMSSP-Auth) to Servers and Server was unable to Authenticate it.

But in the case of “http authsplice on <virtual Service>”, APV was using single TCP connection to complete all the Authentication requests (Request, NTLMSSP-Negotiate, NTLMSSP-Auth). To fix this we have disabled the “Connection Reuse” on the Real Server.

Final configuration on APV to make it compatible with Application access and Windows Authentication is,

- Keeping HTTP AuthSplice to off on Virtual Service
- Disabling Connection Reuse on Real Servers.

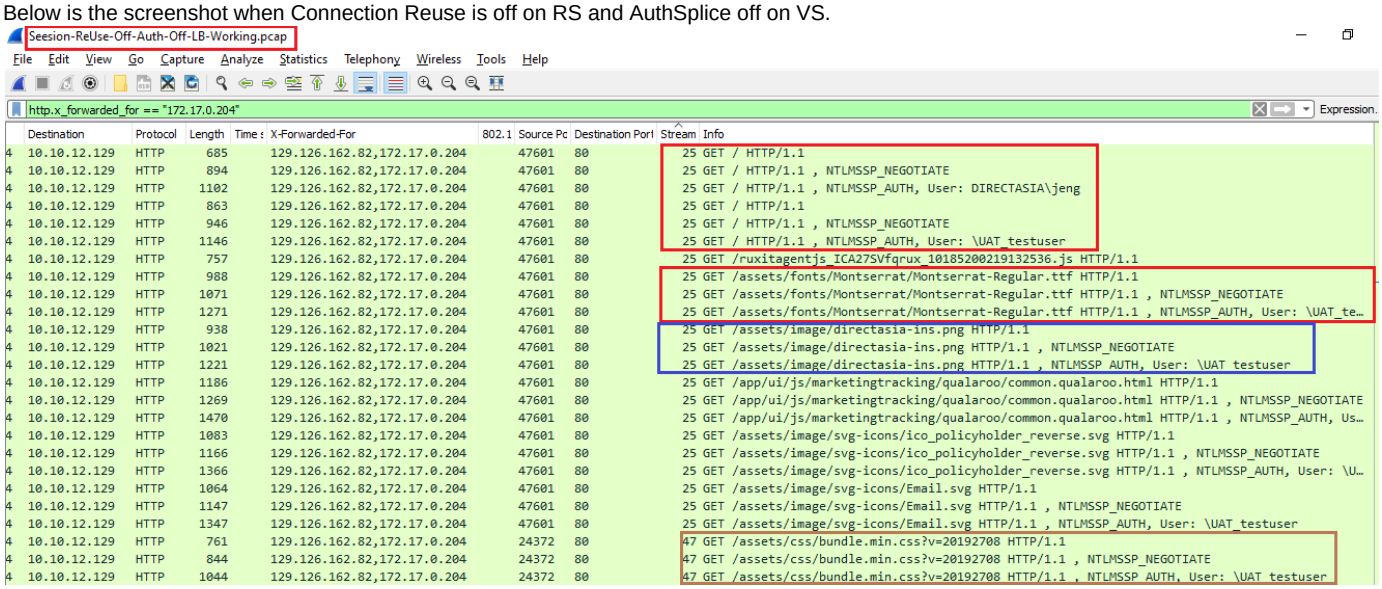
Command to disable Authsplice

http authsplice {on|off} <virtual_service>

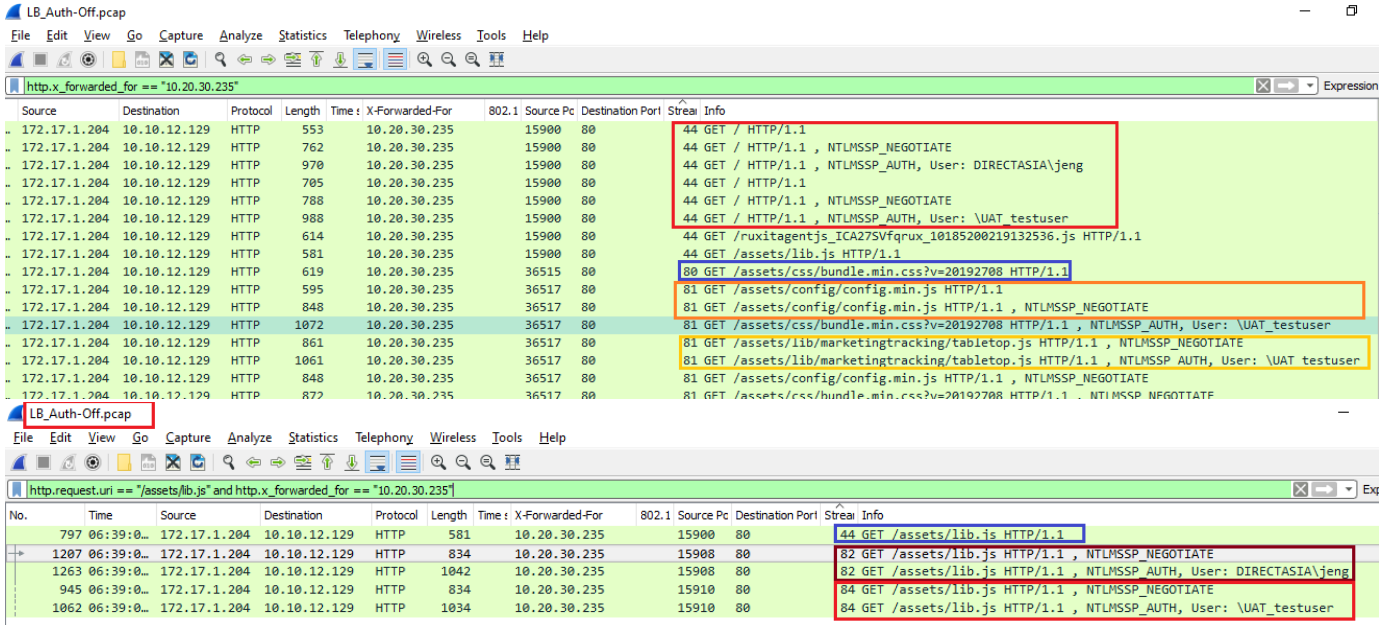
Command to disable Connection Reuse on Real Server

http serverconnreuse real <real_service> off

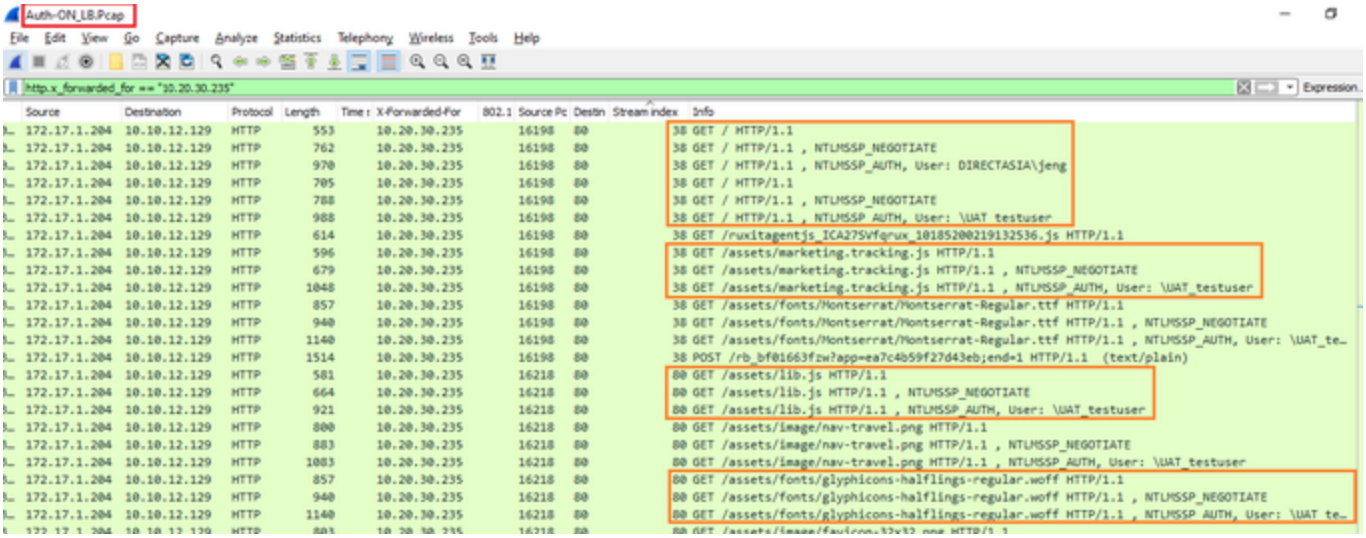
Below is the screenshot when Connection Reuse is off on RS and AuthSplice off on VS.



Below is the screenshot when Connection Reuse is ON on RS and AuthSplice off on VS.



Below is the screenshot when Connection Reuse is ON on RS and AuthSplice ON on VS.



📎 Related articles

https://docs.microsoft.com/en-us/iis/configuration/system.webServer/security/authentication/windowsAuthentication/

- Windows Authentication Issue
- Changes required while using Exchange 2019 as HTTPS Real Server
- Decrypt Packet capture with Session keys
- Unable to turn on AG WebUI
- "Session table not valid" Error on AG